REDSEAL

May 9, 2016

Members, Commission on Enhancing National Cybersecurity
c/o Kevin Kimball, Chief of Staff
Office of the Director
National Institute of Standards and Technology
Department of Commerce
via email: kevin.kimball@nist.gov

Mr. Kimball –

Please share this letter with the members of the Commission on Enhancing National Cybersecurity.

President Obama has charged you with the critically-important task of identifying the steps that our nation must take to enhance cybersecurity in an increasingly dangerous digital world. As discussed at the Commission's inaugural meeting, you are asked to make actionable recommendations for the public and private sectors that address cyber threats today and in the future. Public input will help guide your recommendations.

I applaud the commission's goals and your willingness to undertake this effort. The challenges before you will not have simple solutions. Indeed, billions of dollars are spent every year on cybersecurity products yet breaches continue to happen; they have almost become routine. Every day we learn that solutions can have a short shelf life, and that hackers have managed to stay a few steps ahead of those trying to track them down. Against this backdrop, your work becomes even more important.

As an early investor in cybersecurity startups and now CEO of a cybersecurity analytics company, I encourage you to consider the following modest, but actionable recommendations. Each will help move us forward to an era of cyber best practices.

One: change of perspective

Step one requires a paradigm shift from prevention to inevitability. All of our networks are regularly probed and penetrated by attackers looking for weaknesses. Given the complexity of our networks and the sophistication and persistence of attackers, some of these attacks will be successful. Rather than focusing solely on preventing the unpreventable, we should prepare for the inevitable and make networks resilient so they can operate through an attack and minimize business disruption.

Two: appoint new officers

Step two is to realize that digital resilience is no longer just the responsibility of an organization's IT department. It must be managed at the highest levels of an organization. Businesses and organizations should follow the example of New Orleans and appoint a *chief resilience officer* reporting to the CEO and board executive committee. This role is broader than that of chief information security officers (CISOs) who have traditionally focused on cybersecurity technology. A resilience officer would manage risks and tradeoffs, set priorities, and engage senior decision makers on what is really important for an organization's continuity. Corporate boards need to get involved, too. Every board should be required to include at least one member with cybersecurity experience.

Three: understand the network landscape
Step three is to understand what each network looks like, how it is set up, and how it is constantly changing. Networks, even simple networks, are patchwork structures that grow over time; more end point devices, more storage, more computational power, and more administrative rules. As networks grow, mistakes are made and new attack vectors are opened. If you don't know what you really have, how can you manage it? When you know the extent of your network, you can verify that you are complying with regulations, policies, and industry best practices. You can understand what part of your network might be at risk and respond quickly when any incident does happen.

Four: management through measurement
Step four is to identify clear metrics for resilience and security preparedness. A key tenant of all management training is that you can't manage what you can't measure. Currently, there are many measures of how much activity is going on in a network, how many attacks have been launched, and how many successful defenses have been deployed. But we need to go beyond activity and measure the results of cybersecurity, examine how resilient a network is, and how prepared IT managers are to identify active threats and keep a network operational even during a successful attack.

Five: implement versus reinvent
We generally don't need to invent new standards and regulations. We have many thoughtful public and private sector policies in place from NIST, the Department of Homeland Security, the North American Electric Reliability Corporation, Common Weakness Enumeration group, and others. We need to implement and maintain them to minimize damage to our networks and stay resilient.

Six: address the human factor
Everyone in an organization uses the network. And networks are all interconnected. All it takes is one click on a phishing email and malware is launched, leaving an open door for hackers to enter immediately, in a few months, or even years later. We need to develop a culture of cyber awareness, help people spot hacking techniques, and train them in good security practices. It starts with simple things like changing your passwords regularly. How do we make people cyber aware?

My advice is to stay focused on short term solutions with a long term foundation. The cybersecurity battle will be fought in a changing digital landscape. Today's successful strategies and tactics will be tomorrow's battlefield blunders. With the threat landscape constantly changing, security is an elusive goal. But with a change in perspective, new leadership, and broad cyber awareness, we can be prepared and resilient so that networks that are critical to our economy and civil society can be sustained while the battle rages.

Sincerely,

Ray Rothrock
Chairman and CEO, RedSeal

cc: Kevin Stine, via email to *kevin.stine@nist.gov*
cybercommission@nist.gov